看雪ctf记录第一题

原创

Praise008 于 2017-06-26 16:39:53 发布 349 收藏 1
分类专栏： ctf 文章标签： ctf


```
点击测试程序随便输入提示error后使用ida

根据ida打开搜索error 跳转后f5转换成c代码
```

```
int sub_4011F4()
{
  int v0; // ecx@8
  double v1; // st7@8
  double v2; // st6@8
  double v3; // st6@8
  const CHAR *v5; // [sp-Ch] [bp-28h]@9
  const CHAR *v6; // [sp-8h] [bp-24h]@8
  CHAR String; // [sp+0h] [bp-1Ch]@1
  char v8; // [sp+1h] [bp-1Bh]@3
  char v9; // [sp+2h] [bp-1Ah]@4
  char v10; // [sp+3h] [bp-19h]@5
  int v11; // [sp+18h] [bp-4h]@8
  //获取输入的key
  GetDlgItemTextA(hDlg, 1001, &String, 21);
  //调用这个函数以获得与对话框中的控件相关的标题或文本,1001是指定了要获取其标题的控件的整数标识符,&String指向要接收控件的
  //,21代表要拷到&String的字符串最大长度单位是字节,如果超出就截断.
  Sleep(0x1F4u);     //u是无符号整数,sleep是毫秒作为单位,500毫秒
  if ( strlen(&String) != 4 || String == 48 || v8 == 48 || v9 == 48 || v10 == 48 || String != 49 || v8 != 5
  //逻辑或运算只要有一个为1,先判断输入的字符长度是否为4,不是就跳转到LABEL_11报出密码错误,48 ascii码为0
  //String == 48 || v8 == 48 || v9 == 48 || v10 == 48     字符串1,2,3,4不能为0
  //String != 49 || v8 != 53 第一位为1 第二位为5 确定两位,因为不为1和5报错就可以认为第一位和第二位.
  {
    // Caption值为'CrackMe 2017 CTF v2'
    v6 = Caption;
    goto LABEL_11;
  }
  JUMPOUT(v8 == 53, (char *)&loc_401262 + 1);
  JUMPOUT(0, (char *)&loc_401262 + 1);
  v48CACD();
  //根据上面判断String为第一位,v8第二位,v9第三位,v10第四位密码
  v11 = v9 - v0;
  v1 = (double)v11;  //v1=第三位
  v11 = String - v0;
  v2 = (double)v11;   //v2=第一位
  v11 = v8 - v0;
  v3 = v2 / (double)v11;
  v11 = v10 - v0;
  *(float *)&v11 = (v1 - v3) * (double)v11 * 16.0;
```

```
  //主要算法在上面
  /*for a1 in range(1,10):
    for a2 in range(1,10):
        for a3 in range(1,10):
            for a4 in range(1,10):
                if (a3-(a1/a2))*a4==24:
                    print(a1,a2,a3,a4)*/
  JUMPOUT(v10, v0, (char *)&loc_4012AA + 1);
  JUMPOUT(v10 != v0, (char *)&loc_4012AA + 1);
  v48CB15();
  v6 = aCrackme2017Ctf;
  if ( *(float *)&v11 != 384.0 )      //384/16=24
  {
LABEL_11:
    v5 = Text;
    return MessageBoxA(hWnd, v5, v6, 0);
  }
  v5 = aRegistrationSu;
  return MessageBoxA(hWnd, v5, v6, 0);
}
```

1 1 4 8
1 1 5 6
1 1 7 4
1 1 9 3
1 3 3 9
1 5 5 5
2 1 5 8
2 1 6 6
2 1 8 4
2 2 4 8
2 2 5 6
2 2 7 4
2 2 9 3
.....
9 9 9 3
因为判断长度为4 所以输出4位,而且第一位和第二位为1和5 ,所以匹配1555